Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3
Криптоаналіз афінної біграмної підстановки
Варіант – 1

Виконав:
студент III курсу ФТІ
групи ФБ-95
Чорний Анатолій
Перевірила:
Селюх П. В.

Мета роботи:

Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

Порядок виконання роботи:

1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь. При розв'язуванні порівнянь потрібно коректно обробляти випадок із декількома розв'язками, повертаючи їх усі.
2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).
3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифртексту (розглядаючи пари біграм із п'яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ (a,b) шляхом розв'язання системи (1).
4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.
5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

Хід роботи

1. Спочатку були реалізовані функції знаходження найбільшого спільного кратного, вирішення модулярного рівняння (та вирішення рівняння у загальному випадку).
2. Далі за правилом перетворення були створені функції що переводять біграми у числові значення та навпаки.
3. Після цього наробки з першого лабораторного практикуму були використані для підрахунку найчастіших біграм шифрованного тексту (найчастіші біграми відкритого тексту біли взяті з методичних вказівок).
4. Для відтворення множини ключів були взяті всі можливі співставлення біграм відкритого тексту і біграм тексту шифрованого. Таких співставлень було 25. Для створення системи рівнянь були взяті всі можливі пари співствлень з 25: 625. Для кожної пари була вирішена система рівнянь. Всі корені всіх систем були записані до массиву в єдиному екземплярі (звісно можна було б знайти перетин всіх множин коренів систем, але оскілки таких множин досить багато, було прийняте рішення вирішити питання іншим способом). На виході маємо 23071 можливий ключ.
5. Функція дешифрування тексту представляє собою цикл що декодує текст побіграмно, що дає можливість при зустрічі забороненної біграми прервати ітарацію циклу, що значно збільшило швидкодію. Список забороненних біграм було взято зі статті про частотній аналіз російської мови, та модифіковано з огляду на те що у тексті можуть бути біграми що складаються с останньої букви одного слова та першої букви іншого слова. При досягненні розшифрованним текстом довжини зашифрованного повертається значення відкритого тексту.
6. Основною на мій погляд перепоною був змінений порядок літер в алфавіті при шифруванні тексту (перестановка "ь" та "ы"), що знатно ускладнило процес.

Зашифрований текст:

*лквдвдьышкрбызякиабшачрнвязарчтчлчькзтманэмнязяыбштрпнхтрхрнзтжкккысечамнмпывйвфяжтинфвйвйвсжнпчнмпгущзкыфвйвутсюцзкыкынмотзщбйьыбшхолуычгкицепзкианьуыфллфтыраючькиащзтыфэнкйяпезтнкжкккысечамнмпжэпаычйдбцвсшчмтшслаиятасзбчжйьыбшывлтйэзщбцпцмпщрифкздтеэкктщзархрчосйпрйжклечаккяжюыщяояфскчбяызрчйзчвгзжзычэявсшчтщлжочшызюшхачрнтмнкуфйзбчечвпчнотмнктхеотнчняцзбшрчычбчнкицгщлчькевочфыщяцзреотйсфтбйщялчдечамнмпйарчтчццзтьярняыхашхаытыыздсепцяьаючшзбшзтжмсяачрнвязаозеарчэяицкятчрогцфэкыпэзтйпчаэеэявахыдпдойдкрмпбцмвеэлжочрчщтецрнбяшкуэтыычлчокбцккузбнинепжвининачрнсджяцццаиятчщтецрнбяшквдиабцотияьаццйвычфткюмпьяэяддаьччшызюсяуядсяжутрхбцшчрнфэтзткзтцтеялчакиажчштзмнксябяешщтецрнбяшкуэчцеопнхоьяючбястзырзгьфлуфжмнкецььэтнкфячащжвжяымэвячатьияцзоеязднеэмэйкоевсщыяыяажвычцяучпяэязяшкинвдэякзюнзтмакырцсоушрнецчнкяуялжочознкьызацнкяжсгмпчнвдепйдрчкеэярклнвцычпрычжкнпщюрчньаччквсеокяяорнбччнйцнбшзикзчшклзпеепаопниашчеквдзеязэгцеккьыызацнкшчрнхкнчьхвсфэиащзинэяьяцзчцычжтмэывйвщтецрнбяшктфбйьыемтщцзжеьытнщрпаозвзьнотпанхзайдкрмпбцсрпацрущзлчшклееэхкжяццлтяыбчлуучвзпяэякящяцзэклтвсбцяыыцлтбцдйрцецкзвзвычяквсойюшххолуычннйвбнзеевсоцзпахышчгзючушчядкщрпаозмеяззябчмтмаэзуыйюфэхьбшркбцуэдйуфрняыннйвцяучрнкейпрцккутгщяжйухыксмпкырабцпабштхлтйвчябксогьракыбротхыачрнмнкршчуярачыбяцзрчфяяктфчнвдщтецрнбяшкдфччжшюжачрнвязарчтчучнплзраюьтпнкшчюйзтвйпцдзтофтфэцтнкэофтчнщщккуфпяыцщряжеегщпцбцхкюзгзщырнэяччяыцзыэщрмпбцсрпарчтчбйхярняыжклжььцснкшчэяутпамзгьпнсевсэзфяцзоэцтнвеэззвьдчекеэгызнзтчнпнивучппжкнкэблыибшхязрнпыьарчньччфьстланвеэиэмпрчвьмкеэйкогхчтыыззэивьяньзяфякщтыэзчягшяжпьсжфтщюызкдзтзщачзяюшкзйзлафпэойзьялчуцднеэнпейвязярнбйеплюдфызякиащзачрнвязаозеьхьрнфпечзэгмшчрнйахыбшнрчнмпмэхчйцбйвсчнмпмэьяючбяьярняыцеязочйсхкфпхотнртмэчзкыквипйнктейесолйджкмэшчрзжйеспнмэйчяовытылуычмебцкяюцотноыкиащзфтногзаашятчфяжтгщтщвырчычбчтчжкрйупиажмыяшкмнйврбфяесоркееэллцеиащзцяцзьзмзщяебтцфвебзозяньюжючьвзжчсгьтчэыучрнепйаозделнйааьцяцзэкйэфтйсрнецеопнхоинхыэврцсбчзмтманэмнязяыцзйсиаычищнввдбцкыьярнбяутсюцзкыфпцеэярнкецзкышчднжчюнйпозяыцзнкйсепькжчокбцпцмнйаэккчюжяычягшнвдфкгнкмяфтпаюьукфвецыогзбшучяпхкььоэинрцогэбфтпаюьтпнкэофяачщдвсеофтпаюьукфвмаолпаццнкяжьцсротвжуяддьыцзяквякяяоебхзлзмзгштышспаэтивщзексонвючшкиабшбйчззсеобйлзиротщзфтйсучфжэвдфяпьзеебччищяцзкодпшяюачйкщебччекиабшфяяцмнкыбэкгхчтыгшичкгнккршчтчиншчияцзывьяючбятьюьюаьыкьзаучйзтысюиебчщзечучючькваднеэльачрнвязарчтчйдбйеплюрбучэтийшчрнвцебтцузйджчутеэььсаучоччкиабшебхзбшфтногзйюрбхобятчйцотасбйбччяцегщечеойюрбмэипкйчнезучлчмыбшхыздыяжкфэмпюжфтецжкнкецсспнезнащзбштыфтфэотучиншчияцзовйдзеотечамнклзйяебччекфвйкинвдщыечикфвжяццзебчочьвеслеяздчюзюабйчыикфтщрчащяцзшсиаычицнвввдевфтпаюьукфвйэинбящзещецпйзтжятчхбцяычлуычфтлзньхярнбяшкжкмафпзкфвчьхззгьутчняьнязьянвсяюыьытнотшрычйцсспнмпйаццеяычрьхярнечяыцзчнйвшхнвючшкиачяюцйдбцььэтнкфякэцтзыхынмлзещккмвинзтчхрытнбцйдгмтщцзрньырнсятчкывыгняжйзутйэлчцяцйцнйамврьйпзквдзтмаьпнкэофяйтмпдфыяечювузпебцйснуычфтинрцзтсрсяьыйтсюжяюаяащявьфлфэбйьыичнафпзксоыярнгьтнрцтыяьрнэякпнкшчрнгсиаычицнввдевинзтсолчспейцаыячыбшйдзеэярнкецзрчжйупецйдгмтщцзтыфтецщятыспецяжлчштзщеэтыиылчтчкяяоечеклнжшдэпаычытчбнбйтзиклнязчнйвфэбйьыичжцхтзщфпмавцеыичвззэлзбьзаццицхкпцкяхыозбятчызякиащзфяеыюччажсчащзьянвшхьягнлжчцеофлиххобятчьыдсьышзчягшичрнфэнрчнмпйаццнкпнотсзлчрнссзмоежчыккюнкэбппкйфэуэебзоеыхынмицйдеэккотнчштплнкэотрчнмнмпмэчнйвдэмпкрнхжкиыюзрнечекицяыькеэиыюзрнучиншчияцзовиылчнькяуянпйсбцмнмпзкеэзщйхчащзднеэшдшызюуфачштвснюфязюуфзайдщытчычлждееэкрлрмпбцмвзаючькдфызякиащзачрнвязарчтчсжлжыяызызэтшийвычьывсхкрчызьярнбяшктфссяыкыьярнбяшкчхйдкрэягцшрифшчучлжияшкрбнитятнрцшчрнгятчлаэтмэщяшкиабшсеотбяющузрчычьышсепькейуплеязбярнсятчтажсеэзщйхтщньфпчаыячыбшфтпаюьукфвеэсятчфяучыссбхяпацытыызкьцзтьянввящыбчяыцзпнйввяочьяхыцзицучюкмэвдючюжрьхярнечяыбшрйкщфяжтгщецйсвйпцсбшмпаычфткгнкыкряеыичвзрнпйкщтыызэзэкицбчичжеиажчыккюнкэбмз

яеязговыцзцеотгзякчхучожечгзфтинрцбйзтрнзьфлшхфэычаэгмнкуффтчавяюзаояалсецгщлчькиащз рьцпфэцтбцккэоачрнвязарчтчзайяхялчькбйупбйфчыкпащзстзщиовьфэхьгшмзекчхюыьытнотбцшчу чючцяцзицтллфвычялкшяюаэкйпщрсялкицбчвыфябйщщмнмпзквдевйвюжючнвзщккзеязщышкчхбйрн ночягшрняыдкбцкяцяечикфвсбхятччянарчэясрмэтыфжхяшкйяиаючькнксяучяпкмплйяочрнзтжкшр мпбцсрпарчтчюеэявсепнкэбфяжтгщднинепжвгщтытнвдкрычянйвдфмзьнкщфяесйпхобнжчшчфт ыуычдезецнмяучтпмнфпиайаечфэйсхкрнечжцьяимицрнбчтчнасжнпоебччцеопнхофяжтгщачрнвяза озгкзщпцйпкяяоиыйзбтедсяхынмпаэзхыызйдмусзщяхнфвеэтыычлчокбцккузбнжчуйупучьцотцяьнщ ммпуэфтцежскыназебчечцсецкзйзхоуччяэяеагщтыцзяаесзтвдйэузучнпйсрбчзньныачякуэтырнбчнк сяжцпажэецотноыккрычднмнйвтыожяымэсогефпоемзчйупйпщюйафэхнеэеэйджкицбчвырчычзжю цхырчнааьшыпащявьпнзеэяыяызбшкыозрнотмусзщяхаэбычпабшкытнщммпрбчачяязсьццотцсмнну ычпеепшчеьбяэяшкиабшпкмпдщюевсзьмеязээтыжцзеотлжееинеэнрычщывжккйэфяжзьянвшхфтц ежсрчзнйвтыожяымэдфгефпоемзссиаычицнввджкйсиахыычяктзфятыыякоыечзнзтчхучычньбнзе жкфэкксяйцщщккяжжагефпоеычссяжйзфтцежскыйзччщяикнкяжжаиаычэкуфиахыпнхофяяаяжеы

Ключ: (13, 151)

Розшифрований текст:

многограннуюличностьдостоевскогоможнорассматриватьсчетырехсторонкакписателякакневро тикакакмыслителяэтикаикакгрешникакакжеразобратьсявэтойневольносмущающейнассложност инаименееспоренонкакписательместоеговодномрядусшекспиромбратьякарамазовывеличайшийром анизвсехкогдалибонаписанныхалегендаовеликоминквизитореодноизвысочайшихдостижениймирово йлитературыпереоценитькотороеневозможноксожалениюпередпроблемойписательскоготворчес твапсихоанализдолженсложитьоружиедостоевскийскореевсегоуязвимкакморалистпредставляяег очеловекомвысоконравственнымнатомосновaниичтотолькототдостигаетвысшегонравственного совершенствактопрошелчерезглубочайшиебездныгреховностимыигнорируемодносоображениеведь нравственнымявляетсячеловекреагирующийуженавнутреннеиспытываемоеискушениеприэтомему неподдаваяськтожепопеременноготрешиттораскаиваясьставитсебевысокиенравственныецелито голегкоупрекнутьвтомчтоонслишкомудобнодлясебястроитсвоюжизньоннеисполняетосновногопри нципанравственностинеобходимостиотречениявтовремякакнравственныйобразжизнивпрактичес кихинтересахвсегочеловечестваэтимоннапоминаетварваровэпохипереселениянародовварваровубив авшихизатемкаявшихсявэтомтакчтопокаяниестановилосьтехническимпримеромрасчищавшимпу тькновымубийстваматакжепоступаливангрозныйэтасделкассовестьюхарактернаярусскаячертадо статочнобесславениконечныйитогнравственнойборьбыдостоевскогопослеисступленнойборьбывои мяпримиренияпритязанийпервичныхпозывовиндивидастребованиямичеловеческогообществаонвыну жденнорегрессируеткподчинениюмирскомуидуховномуавторитетукпоклонениюцарюихристианско мубогукрусскомумелкодушномунационализмукчемуменеезначительныеумыпришлисгораздоменьшим иусилиямичемонвэтомслабоеместобольшойличностидостоевскийупустилвозможностьстатьучит елемиосвободителемчеловечестваприсоединилсяктюремщикамкультурабудущегонемногимбудете муобязанавэтомповсейвероятностипроявилсяегоневрозиззакоторогоонибылосужденнатакуюнеуда чупомощипостиженияисилелюбвиклюдямемубылоткрытдругойапостольскийпутьслужениянампре дставляетсяотталкивающимрассматриваниедостоевскоговкачествегрешникаилипреступниканоэ тоотталкиваниенедолжноосновыватьсянаобывательскойоценкепреступникавыявитьподлиннуюм отивациюпреступлениянедолгодляпреступникасущественныдвечертыбезграничноесебялюбиеисиль наядеструктивнаясклонностьобщимдляобеихчертипредпосылкойдляихпроявленийявляетсябезлюбо вностьнехваткаэмоциональнооценочногоотношениякчеловекутутсразувспоминаешьпротивополо жноеэтомуудостоевскогоегобольшуюпотребностьвлюбвиегоогромнуюспособностьлюбитьпрояви вшуюсявегосверхдоброteипозволявшуюемулюбитьипомогатьтамгдеонимелбыправоненавидетьимс титьнапримерпоотношениюкегопервойженеиеелюбовникунотогдавозникаетвопросоткудаприходи

тсоблазнпричислениядостоевскогокпреступникамответиззавыбораегосюжетовэтопреимуществе ннонасильникиубийцыэгоцентрическиехарактерычтосвидетельствуетосуществованиитакихсклон ностейвеговнутреннеммиреатакжеиззанекоторыхфактовегожизнистрастиегоказартнымиграмм ожетбытьсексуальногорастлениянезрелойдевочкиисповедьэтопротиворечиеразрешаетсяследующ имобразомсильнаядеструктивнаяустремленностьдостоевскогокотораямоглабысделатьегопресту пникомбылавегожизнинаправленаглавнымобразомнасамогосебявовнутрьвместотогочтобыизнутр иитакимобразомвыразилассьвмазохизмеичувствевинывсетакивеголичностинемалоисадистическихч ертвыявляющихсявегораздражительностимучительстванетерпимостидажепоотношениюклюбим ымлюдяматакжевегоманереобращениясчитателемитаквмелочахонсадиствовневажномсадистпо отношениюксамомусебеследовательномазохистиэтомягчайшийдобродушнейшийвсегдаготовыйпо мочьчеловеквсложнойличностидостоевскогомывыделилитрифактораодинколичественныйидвакач ественныхегочрезвычайноповышеннуюаффективностьегоустремленностькперверзиикотораядолж набылапривестиегоксадомазохизмуилисделатьпреступникомиегонеподдающееесяанализутворческо едарованиетакоесочетаниевполнемоглобысуществоватьибезневрозаведьбываютжестопроцентны емазохистыбезналичияневрозовпосоотношениюсилпритязаниипервичныхпозывовипротивоборству ющихимторможенийприсоединяясюдавозможностисублимированиядостоевскоговсеещеможнобы лобыотнестикразрядуимпульсивныххарактеровноположениевещейзатемняетсяналичиемневрозане обязательногокакбылосказаноприданныхобстоятельствахновсежевозникающеготемскореечемнас ыщеннееосложнениеподлежащеесосторонычеловеческогояпреодолениюневрозэтотолькознактогоч тоятакойсинтезнеудалсячтооноприэтойпопыткепоплатилосьсвоимединствомвчемжевстрогомсм ыслепроявляетсяневроздостоевскийназывалсебясамидругиетакжесчиталиегоэпилептикомнатомо снованиичтоонбылподвержентяжелымприпадкамсопровождавшимисяпотерейсознаниясудорогам иипоследующимупадочнымнастроениемвесьмаверояпочтоэтатакназываемаяэпилепсиябылалишь симптомомегоневрозакоторыйвтакомслучаеследуетопределитькакистероэпилепсиютоестькактя желуюистериюутверждатьэтосполнойуверенностьюнельзяподвумпричинамвопервыхпотомучтод атыанамнезическихприпадковтакназываемойэпилепсиидостоевскогонедостаточныиненадежныав оторыхпотомучтопониманиесвязанныхсэпилептоидныприпадкамиболезненныхсостоянийостае тсянеясныма

Висновки: в ході виконання компьютерного практикуму мною були досліджені методи розшифрування тексту зашифрованного способом афінної біграмної підстановки. Були відтворенні функції для вирішення систем модулярних рівнянь що можуть повертати всі можливі корені системи. Також були проаналізовані можливі критерії відкритого тексту, та з огляду на швидкодію було обрано метод заборонених біграм.